US006253193B1

(12) **United States Patent**
Ginter et al.

(10) **Patent No.: US 6,253,193 B1**
(45) **Date of Patent: Jun. 26, 2001**

(54) **SYSTEMS AND METHODS FOR THE SECURE TRANSACTION MANAGEMENT AND ELECTRONIC RIGHTS PROTECTION**

(75) Inventors: **Karl L. Ginter**, Beltsville; **Victor H. Shear**, Bethesda, both of MD (US); **Francis J. Spahn**, El Cerrito; **David M. Van Wie**, Sunnyvale, both of CA (US)

(73) Assignee: **InterTrust Technologies Corporation**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/208,017**

(22) Filed: **Dec. 9, 1998**

Related U.S. Application Data

(63) Continuation of application No. 08/964,333, filed on Nov. 4, 1997, now Pat. No. 5,982,891, which is a continuation of application No. 08/388,107, filed on Feb. 13, 1995, now abandoned.

(51) **Int. Cl.**[7] **H04L 9/32**
(52) **U.S. Cl.** **705/57**; 705/52
(58) **Field of Search** 705/51, 52, 56, 705/57; 380/201–203; 386/94, 124

(56) **References Cited**

U.S. PATENT DOCUMENTS

3,573,747	4/1971	Adams et al. .
3,609,697	9/1971	Blevins .
3,796,830	3/1974	Smith .
3,798,359	3/1974	Feistel .
3,798,360	3/1974	Feistel .
3,798,605	3/1974	Feistel .
3,806,882	4/1974	Clarke .
3,829,833	8/1974	Freeny .
3,906,448	9/1975	Henriques .
3,911,397	10/1975	Freeny .
3,924,065	12/1975	Freeny .
3,931,504	1/1976	Jacoby .
3,946,220	3/1976	Brobeck et al. .

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

62-241061	12/1984	(BE) .
9 004 79	12/1984	(BE) .
3803982A1	1/1990	(DE) .

(List continued on next page.)

OTHER PUBLICATIONS

David Arneke and Donna Cunningham, Document from the Internet: AT&T encryption system protects information services, (News Release), Jan. 9, 1995, 1 page.

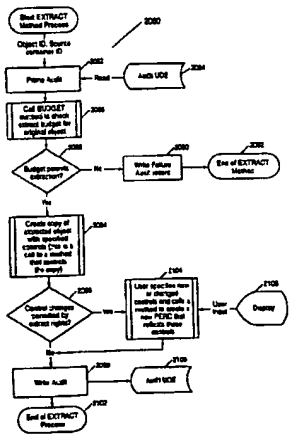
(List continued on next page.)

Primary Examiner—Gilberto Barrón, Jr.
(74) *Attorney, Agent, or Firm*—Finnegan, Henderson, Farabow, Garrett & Dunner L.L.P.

(57) **ABSTRACT**

The present invention provides systems and methods for secure transaction management and electronic rights protection. Electronic appliances such as computers equipped in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Distributed and other operating systems, environments and architectures, such as, for example, those using tamper-resistant hardware-based processors, may establish security at each node. These techniques may be used to support an all-electronic information distribution, for example, utilizing the "electronic highway."

72 Claims, 146 Drawing Sheets



U.S. PATENT DOCUMENTS

3,956,615	5/1976	Anderson et al. .	
3,958,081	5/1976	Ehrsam et al. .	
3,970,992	7/1976	Boothroyd et al. .	
4,048,619	9/1977	Forman, Jr. et al. .	
4,071,911	1/1978	Mazur .	
4,112,421	9/1978	Freeny .	
4,120,030	10/1978	Johnstone .	
4,163,280	7/1979	Mori et al. .	
4,168,396	9/1979	Best .	
4,196,310	4/1980	Forman et al. .	
4,200,913	4/1980	Kuhar et al. .	
4,209,787	6/1980	Freeny .	
4,217,588	8/1980	Freeny .	
4,220,991	9/1980	Hamano et al. .	
4,232,193	11/1980	Gerard .	
4,232,317	11/1980	Freeny .	
4,236,217	11/1980	Kennedy .	
4,253,157	2/1981	Kirschner et al. .	
4,262,329	4/1981	Bright et al. .	
4,265,371	5/1981	Desai et al. .	
4,270,182	5/1981	Asija .	
4,278,837	7/1981	Best .	
4,305,131	12/1981	Best .	
4,306,289	12/1981	Lumley .	
4,309,569	1/1982	Merkle .	
4,319,079	3/1982	Best .	
4,323,921	4/1982	Guillou .	
4,328,544	5/1982	Baldwin et al. .	
4,337,483	6/1982	Guillou .	
4,361,877	11/1982	Dyer et al. .	
4,375,579	3/1983	Davida et al. .	
4,433,207	2/1984	Best .	
4,434,464	2/1984	Suzuki et al. .	
4,442,486	4/1984	Mayer .	
4,446,519	5/1984	Thomas .	
4,454,594	6/1984	Heffron et al. .	
4,458,315	7/1984	Uchenick .	
4,462,076	7/1984	Smith .	
4,462,078	7/1984	Ross .	
4,465,901	8/1984	Best .	
4,471,163	9/1984	Donald et al. .	
4,484,217	11/1984	Block et al. .	
4,494,156	1/1985	Kadison et al. .	
4,513,174	4/1985	Herman .	
4,528,588	7/1985	Lofberg .	
4,528,643	7/1985	Freeny .	
4,553,252	11/1985	Egendorf .	
4,558,176	12/1985	Arnold et al. .	
4,558,413	12/1985	Schmidt et al. .	
4,562,306	12/1985	Chou et al. .	
4,562,495	12/1985	Bond et al. .	
4,577,289	3/1986	Comerford et al. .	
4,584,641	4/1986	Guglielmino .	
4,588,991	5/1986	Atalla .	
4,589,064	5/1986	Chiba et al. .	
4,593,353	6/1986	Pickholtz .	
4,593,376	6/1986	Volk .	
4,595,950	6/1986	Lofberg .	
4,597,058	6/1986	Izumi et al. .	
4,634,807	1/1987	Chorley et al. .	
4,644,493	2/1987	Chandra et al. .	
4,646,234	2/1987	Tolman et al. .	
4,652,990	3/1987	Pailen et al. .	
4,658,093	4/1987	Hellman .	
4,670,857	6/1987	Rackman .	
4,672,572	6/1987	Alsberg .	
4,677,434	6/1987	Fascenda .	
4,680,731	7/1987	Izumi et al. .	
4,683,553	7/1987	Mollier .	
4,685,056	8/1987	Barnsdale et al. .	
4,688,169	8/1987	Joshi .	
4,691,350	9/1987	Kleijne et al. .	
4,696,034	9/1987	Wiedemer .	
4,700,296	* 10/1987	Palmer, Jr. et al.	705/32
4,701,846	10/1987	Ikeda et al. .	
4,712,238	12/1987	Gilhousen et al. .	
4,713,753	12/1987	Boebert et al. .	
4,740,890	4/1988	William .	
4,747,139	5/1988	Taaffe .	
4,757,533	7/1988	Allen et al. .	
4,757,534	7/1988	Matyas et al. .	
4,768,087	8/1988	Taub et al. .	
4,791,565	12/1988	Dunham et al. .	
4,796,181	1/1989	Wiedemer .	
4,799,156	1/1989	Shavit .	
4,807,288	2/1989	Ugon et al. .	
4,817,140	3/1989	Chandra et al. .	
4,823,264	4/1989	Deming .	
4,827,508	5/1989	Shear .	
4,858,121	8/1989	Barber et al. .	
4,864,494	9/1989	Kobus .	
4,866,769	* 9/1989	Karp	380/56
4,868,877	9/1989	Fischer .	
4,903,296	2/1990	Chandra et al. .	
4,924,378	5/1990	Hershey et al. .	
4,930,073	5/1990	Cina .	
4,949,187	8/1990	Cohen .	
4,975,647	* 12/1990	Downer et al.	713/168
4,977,594	12/1990	Shear .	
4,999,806	3/1991	Chernow et al. .	
5,001,752	3/1991	Fischer .	
5,005,122	4/1991	Griffin et al. .	
5,005,200	4/1991	Fischer .	
5,010,571	4/1991	Katznelson .	
5,023,907	6/1991	Johnson et al. .	
5,047,928	9/1991	Wiedemer .	
5,048,085	9/1991	Abraham et al. .	
5,050,213	9/1991	Shear .	
5,091,966	2/1992	Bloomberg et al. .	
5,103,392	4/1992	Mori et al. .	
5,103,476	4/1992	Waite et al. .	
5,111,390	5/1992	Ketcham .	
5,119,493	6/1992	Janis et al. .	
5,128,525	7/1992	Stearns et al. .	
5,136,643	8/1992	Fischer .	
5,136,646	8/1992	Haber .	
5,136,647	8/1992	Haber .	
5,136,716	8/1992	Harvey et al. .	
5,146,575	9/1992	Nolan .	
5,148,481	9/1992	Abraham et al. .	
5,155,680	10/1992	Wiedemer .	
5,163,091	11/1992	Graziano et al. .	
5,168,147	12/1992	Bloomberg .	
5,185,717	2/1993	Mori .	
5,201,046	4/1993	Goldberg et al. .	
5,201,047	4/1993	Maki et al. .	
5,208,748	5/1993	Flores et al. .	
5,214,702	5/1993	Fischer .	
5,216,603	6/1993	Flores et al. .	
5,221,833	6/1993	Hecht .	
5,222,134	6/1993	Waite et al. .	
5,224,160	6/1993	Paulini et al. .	
5,224,163	6/1993	Gasser et al. .	
5,235,642	8/1993	Wobber et al. .	
5,245,165	9/1993	Zhang .	
5,247,575	9/1993	Sprague et al. .	
5,260,999	11/1993	Wyman .	
5,263,158	11/1993	Janis .	
5,265,164	11/1993	Matyas et al. .	
5,276,735	1/1994	Boebert et al. .	
5,280,479	1/1994	Mary .	

5,285,494	2/1994	Sprecher et al. .
5,301,231	4/1994	Abraham et al. .
5,311,591	5/1994	Fischer .
5,319,705	6/1994	Halter et al. .
5,319,785	6/1994	Halter et al. .
5,337,360	8/1994	Fischer .
5,341,429	8/1994	Stringer et al. .
5,343,527	8/1994	Moore et al. .
5,347,579	9/1994	Blandford .
5,351,293	9/1994	Michener .
5,355,474	10/1994	Thuraisngham et al. .
5,373,561	12/1994	Haber et al. .
5,390,247	2/1995	Fischer .
5,390,330	2/1995	Talati .
5,392,220	2/1995	van der Hamer et al. .
5,392,390	2/1995	Crozier .
5,394,469	2/1995	Nagel et al. .
5,410,598	4/1995	Shear .
5,412,717	5/1995	Fischer .
5,421,006	5/1995	Jablon .
5,422,953	6/1995	Fischer .
5,428,606	6/1995	Moskowitz .
5,438,508	8/1995	Wyman .
5,442,645	8/1995	Ugon .
5,444,779	8/1995	Daniele .
5,449,895	9/1995	Hecht et al. .
5,449,896	9/1995	Hecht et al. .
5,450,493	9/1995	Maher .
5,453,601	9/1995	Rosen .
5,453,605	9/1995	Hecht et al. .
5,455,407	10/1995	Rosen .
5,455,861	10/1995	Faucher et al. .
5,455,953	10/1995	Russell .
5,457,746	10/1995	Dolphin .
5,463,565	10/1995	Cookson et al. .
5,473,687	12/1995	Lipscomb et al. .
5,473,692	12/1995	Davis .
5,479,509	12/1995	Ugon .
5,485,622	1/1996	Yamaki .
5,491,800	2/1996	Goldsmith et al. .
5,497,479	3/1996	Hornbuckle .
5,497,491	3/1996	Mitchell et al. .
5,499,298	3/1996	Narasimhalu et al. .
5,504,757	4/1996	Cook et al. .
5,504,818	4/1996	Okano .
5,504,837	4/1996	Griffeth et al. .
5,508,913	4/1996	Yamamoto et al. .
5,509,070	4/1996	Schull .
5,513,261	4/1996	Maher .
5,517,518	5/1996	Rosen .
5,530,235	6/1996	Stefik et al. .
5,530,752	6/1996	Rubin .
5,533,123	7/1996	Force et al. .
5,534,975	7/1996	Stefik et al. .
5,537,526	7/1996	Anderson et al. .
5,539,735	7/1996	Moskowitz .
5,539,828	7/1996	Davis .
5,550,971	8/1996	Brunner et al. .
5,553,282	9/1996	Parrish et al. .
5,557,518	9/1996	Rosen .
5,563,946	10/1996	Cooper et al. .
5,568,552	10/1996	Davis .
5,572,673	11/1996	Shurts .
5,592,549	1/1997	Nagel et al. .
5,606,609	2/1997	Houser et al. .
5,613,004	3/1997	Cooperman et al. .
5,621,797	4/1997	Rosen .
5,629,980	5/1997	Stefik et al. .
5,633,932	5/1997	Davis .
5,634,012	5/1997	Stefik et al. .
5,636,292	6/1997	Rhoads .
5,638,443	6/1997	Stefik .
5,638,504	6/1997	Scott et al. .
5,640,546	6/1997	Gopinath .
5,655,077	8/1997	Jones et al. .
5,687,236	11/1997	Moskowitz et al. .
5,689,587	11/1997	Bender .
5,692,180	11/1997	Lee .
5,710,834	1/1998	Rhoads .
5,740,549	4/1998	Reilly et al. .
5,745,604	4/1998	Rhoads .
5,748,763	5/1998	Rhoads .
5,748,783	5/1998	Rhoads .
5,754,849	5/1998	Dyer et al. .
5,758,152	5/1998	LeTourneau .
5,765,152	6/1998	Erickson .
5,768,426	6/1998	Rhoads .

FOREIGN PATENT DOCUMENTS

0 084 441 A1	7/1983	(EP) .
0 128 672 A1	12/1984	(EP) .
0 135 422 A1	3/1985	(EP) .
0 180 460 A1	5/1986	(EP) .
0 370 146 A1	5/1990	(EP) .
0 399 822 A2	11/1990	(EP) .
0 421 409 A2	4/1991	(EP) .
0 456 386 A2	11/1991	(EP) .
0 469 864 A2	2/1992	(EP) .
0 469 864 A3	2/1992	(EP) .
0 565 314 A2	10/1993	(EP) .
0 593 305 A2	4/1994	(EP) .
0 651 554 A1	5/1995	(EP) .
0 668 695 A2	8/1995	(EP) .
0 668 695 A3	8/1995	(EP) .
0 725 376 A2	1/1996	(EP) .
0 695 985 A1	2/1996	(EP) .
0 696 798 A1	2/1996	(EP) .
0 715 243 A1	6/1996	(EP) .
0 715 244 A1	6/1996	(EP) .
0 715 245 A1	6/1996	(EP) .
0 715 246 A1	6/1996	(EP) .
2136175	9/1984	(GB) .
2264796A	9/1993	(GB) .
2294348	4/1996	(GB) .
2295947	6/1996	(GB) .
57-726	5/1982	(JP) .
62-225059	8/1987	(JP) .
62-241061	10/1987	(JP) .
1-068835	3/1989	(JP) .
64-68835	3/1989	(JP) .
2-242352	9/1990	(JP) .
2-247763	10/1990	(JP) .
2-294855	12/1990	(JP) .
4-369068	12/1992	(JP) .
5-181734	7/1993	(JP) .
5-257783	10/1993	(JP) .
5-268415	10/1993	(JP) .
6-175794	6/1994	(JP) .
6-215010	8/1994	(JP) .
7-056794	3/1995	(JP) .
7-084852	3/1995	(JP) .
7-141138	6/1995	(JP) .
7-200317	8/1995	(JP) .
7-200492	8/1995	(JP) .
7-244639	9/1995	(JP) .
8-137795	5/1996	(JP) .
8-152990	6/1996	(JP) .
8-105298	7/1996	(JP) .
8-185292	7/1996	(JP) .
WO 85/02310	5/1985	(WO) .
WO 85/03584	8/1985	(WO) .
WO 90/02382	3/1990	(WO) .

WO 92/06438	4/1992	(WO) .
WO 92/22870	12/1992	(WO) .
WO 93/01550	1/1993	(WO) .
WO 94/01821	1/1994	(WO) .
WO 94/03859	2/1994	(WO) .
WO 94/06103	3/1994	(WO) .
WO 94/16395	7/1994	(WO) .
WO 94/18620	8/1994	(WO) .
WO 94/22266	9/1994	(WO) .
WO 94/27406	11/1994	(WO) .
WO 95/14289	5/1995	(WO) .
WO 96/00963	1/1996	(WO) .
WO 96/03835	2/1996	(WO) .
WO 96/05698	2/1996	(WO) .
WO 96/06503	2/1996	(WO) .
WO 96/13013	5/1996	(WO) .
WO 96/21192	7/1996	(WO) .
WO 96/24092	8/1996	(WO) .
WO 97/03423	1/1997	(WO) .
WO 97/07656	3/1997	(WO) .
WO 97/32251	9/1997	(WO) .
WO 97/48203	12/1997	(WO) .

OTHER PUBLICATIONS

Claude Baggett, Cable's Emerging Role in the Information Superhighway, Cable Labs, (undated) 13 slides.

Theodore Sedgwick Barassi, Document from Internet: The Cybernotary: Public Key Registration and Certification and Authentication of International Legal Transactions, (undated), 4 pages.

Hugh Barnes, e–mail to Henry LaMuth, subject: George Gilder articles, May 31, 1994, 2 pages.

Comments in the Matter of Public Hearing and Request for Comments on the International Aspects of the National Information Infrastructure, Before the Department of Commerce, Aug. 12, 1994, pp. 1–15 (comments of Dan Bart).

Michael Baum, "Worldwide Electronic Commerce: Law, Policy and Controls Conference," program details, Nov. 11, 1993, 18 pages.

Robert M. Best, Preventing Software Piracy With Crypto–Microprocessors, Digest of Papers, VLSI: New Architectural Horizons, Feb. 1980, pp. 466–469.

Richard L. Bisbey, II and Gerald J Popek, Encapsulation: An Approach to Operating System Security, (USC/Information Science Institute, Marina Del Rey, CA) Oct. 1973, pp. 666–675.

Rolf Blom, Robert Forchheimer, et al. Encryption Methods in Data Networks, Ericsson Technics, No. 2, Stockholm, Sweden, 1978.

Rick E. Bruner, Document from the Internet: PowerAgent, NetBot help advertisers reach Internet shoppers, Aug. 1997, 3 pages.

Denise Caruso, Technology, Digital Commerce: 2 plans for watermarks, which can bind proof of authorship to electronic works., N.Y. Times, Aug. 7, 1995, p. D5.

A.K. Choudhury, N. F. Maxemchuck, et al., Copyright Protection for Electronic Publishing Over Computer Networks, (AT&T Bell Laboratories, Murray Hill N. J.) Jun. 1994, 17 pages.

Tim Clark, Ad service gives cash back, <www.news.com,/News/Item/0,4,13050,00.html> (visited Aug. 4, 1997) 2 pages.

Donna Cunningham, David Arneke, et al., Document from the Internet: AT&T, VLSI Technology join to improve info highway security, (News Release) Jan., 31, 1995, 3 pages.

Lorcan Dempsey and Stuart Weibel, The Warwick Metadata Workshop: A Framework for the Deployment of Resource Description, D–Lib Magazine, Jul., 15, 1996.

Dorothy E. Denning and Peter J Denning, Data Security, 11 Computing Surveys No. 3, Sep. 1979, pp. 227–249.

Whitfield Diffie and Martin E. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, vol. 22, No. 6, Nov. 1976, pp. 644–651.

Whitfield Diffie and Martin E. Hellman, Privacy and Authentication: An Introduction to Cryptography, Proceedings of the IEEE, vol. 67, No. 3, Mar. 1979 pp. 397–427.

Stephen R. Dusse and Burton S. Kaliski, A Cryptographic Library for the Motorola 56000,, Advances in Cryptology–Proceedings Eurocrypt 90, (I.M. Damgard, ed., Springer–Verlag) 1991, pp. 230–244.

Esther Dyson, Intellectual Value, Wired Magazine, Jul. 1995, pp. 136–141 and 182–183 (This article is not prior art.).

Science, space and technology, Hearing before Subcomm. on Technology, Environment, ad Aviation, May 26, 1994 (testimony of D. Linda Garcia).

James Gleick, Dead as a Dollar, The New York Times Magazine, Jun. 16, 1996, Sect. 6, pp. 26–30, 35, 42, 50, 54.

Fred Greguras, Document from Internet: Softic Symposium '95, Copyright Clearances and Moral Rights, Dec. 11, 1995, 3 pages.

Louis C. Guillou, Smart Cards and Conditional Access, Advances in Cryptography—Proceedings of EuroCrypt 84 (T. Beth et al, Ed., Springer–Verlag) 1985, pp. 480–490.

Harry H. Harman, Modern Factor Analysis, Third Edition Revised, University of Chicago Press, Chicago and London, 1976.

Amir Herzberg and Shlomit S. Pinter, Public Protection of Software, ACM Transactions on Computer Systems, vol. 5, No. 4, Nov. 1987, pp. 371–393.

Jud Hofmann, Interfacing the NII to User Homes, (Consumer Electronic Bus Committee) NIST, Jul. 1994, 12 slides.

Jud Hofmann, Interfacing the NII to User Homes, Electronic Industries Association, (Consumer Electronic Bus Committee) (undated), 14 slides.

Stannie Holt, Document from the Internet: Start–up promises user confidentiality in Web marketing service, InfoWorld Electric News (updated Aug. 13, 1997).

Jay J. Jiang and David W. Conrath, A concept–based Approach to Retrieval from an Electronic Industrial Directory, International Journal of Electronic Commerce, vol. 1, No. 1 (fall 1966) pp. 51–72.

Debra Jones, Document from the Internet: Top Tech Stories, PowerAgent Introduces First Internet 'Informediary' to Empower and Protect Consumers, (updated Aug. 13, 1997) 3 pages.

kevin Kelly, E–Money, Whole Earth Review, Summer 1993,, pp. 40–59.

Stephen Thomas Kent, Protecting Externally Supplied Software in Small Computers, (MIT/LCS/TR–255) Sep. 1980 254 pages.

David M. Kristol, Steven H. Low and Nicholas F. Maxemchuk, Anonymous Internet Mercantile Protocol, (AT&T Bell Laboratories, Murray Hill, NJ) Draft: Mar. 17, 1994.

Carl Lagoze, The Warwick Framework, A Container Architecture for Diverse Sets of Metadata, D–Lib Magazine, Jul./Aug. 1996.